

Free randomness can be amplified

Roger Colbeck^{1,*} and Renato Renner^{2,†}

¹*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada.*

²*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland.*

(Dated: 17th November 2011)

Are there fundamentally random processes in nature? Theoretical predictions, confirmed experimentally, such as the violation of Bell inequalities, point to an affirmative answer. However, these results are based on the assumption that measurement settings can be chosen freely at random, so assume the existence of perfectly free random processes from the outset. Here we consider a scenario in which this assumption is weakened and show that partially free random bits can be amplified to make arbitrarily free ones. More precisely, given a source of random bits whose correlation with other variables is below a certain threshold, we propose a procedure for generating fresh random bits that are virtually uncorrelated with all other variables. We also conjecture that such procedures exist for any non-trivial threshold. Our result is based solely on the no-signalling principle, which is necessary for the existence of free randomness.

I. INTRODUCTION

Physical theories enable us to make predictions. We can ask “what would happen if...” and reason about the answer, even in scenarios that would be virtually impossible to set up in reality [1]. Each scenario corresponds to a choice of parameters, and it is usually implicitly assumed that any of the possible choices can be made—the theory prescribes the subsequent behaviour in every case. One of the main aims of this paper is to identify (minimal) conditions under which such choices can be made freely, i.e., such that they are uncorrelated with any pre-existing values (in a precise sense described later).

The ability to make free choices is important to establish symmetries, on which physical theories can be based. For example, the concept of an electron is based on the implicit assumption that we could pick any of the electrons in the universe and find the same properties (such as its mass). More precisely, given a set of particles that are experimentally indistinguishable, the assumption that we can sample freely from this set establishes a symmetry between them. Following arguments by de Finetti [2, 3], this symmetry implies that we can treat these particles as independent particles of the same type.

A scenario in which making free random choices is particularly relevant is in the context of Bell’s theorem. Here, the distribution arising from measurements, chosen freely from a given set, on an entangled state is used to conclude that quantum correlations cannot be reproduced by a local hidden variable theory [1, 4]. Dropping the assumption that the measurement settings are freely chosen opens a loophole, rendering the conclusion invalid. In particular, if one instead imagines that the settings were determined by events in the past, then it is easy to explain Bell inequality violations with a local classical model. However, one can ask whether the free

choice assumption can be relaxed, allowing for correlations between the measurement settings and other, possibly hidden, variables, but without allowing their complete pre-determination. This has been studied in recent work [5–9] which shows that if the choice of measurement settings is not sufficiently free then particular quantum correlations can be explained with a local classical model.

This raises the question of whether established concepts in physics are rendered invalid if one relaxes the (standard) assumption that the experimenters’ choices are perfectly free. One might imagine, for example, an experimenter who tries to generate free uniform bits, but (unbeknown to them) these bits can be correctly guessed with a probability of success greater than 1/2 using other (pre-existing) parameters. In this paper, we show that partially free random bits can be used to produce arbitrarily free ones. This implies that a relaxed free choice assumption is sufficient to establish all results derived under the assumption of virtually perfect free choices.

To arrive at this conclusion we need to make one assumption about the structure of any underlying physical theory, namely that it is no-signalling, which essentially implies that local parameters are sufficient to make any possible predictions within the theory. As we explain in Appendix C, it turns out that this assumption is necessary in order that perfectly free choices can be consistently incorporated within the theory.

II. PRELIMINARIES

In order to describe our result in detail, we need a precise notion of what partially free randomness means. Our notion is based on Bell’s [1], and we formulate it in terms of *spacetime variables* (SVs) [10], which means that each variable is associated with a spacetime coordinate. This coordinate is to be interpreted as the location in spacetime at which the random variable is available. (We can also treat random variables that are available within a region of spacetime by defining a set of SVs that are copies of the original random variable with different spacetime

*rcolbeck@perimeterinstitute.ca

†renner@phys.ethz.ch

coordinates.)

For a particular SV, X , we say that X is *perfectly free* (with respect to a set of SVs Γ) if it is uniformly distributed and uncorrelated with all SVs in Γ_X , the subset of SVs from Γ that lie outside the future lightcone of X . This definition captures the idea that X is free if there is no reference frame in which it is correlated with variables in its past. Note that it also includes that X is uniformly distributed. While, in other contexts, it may be useful to separate these concepts, in the present work such a distinction is not needed.

We also need a notion of partial freedom. We say that X is ε -free (with respect to Γ) if it is ε -close (in variational distance) to being perfectly free, i.e. if

$$D(P_{X\Gamma_X}, P_{\bar{X}} \times P_{\Gamma_X}) \leq \varepsilon, \quad (1)$$

where $P_{\bar{X}}$ denotes the uniform distribution on X . We use the *variational distance*, defined by $D(P_X, Q_X) := \frac{1}{2} \sum_x |P_X(x) - Q_X(x)|$, as our measure of closeness. It is chosen because of its operational significance: if two distributions have variational distance at most ε , then the probability that we ever notice a difference between them is at most ε . (A note on notation: we use lower case to denote particular instances of upper case SVs.) As an example, if a uniformly random bit X is correlated to a pre-existing bit W such that $P_{X|W=0}(0) = \frac{3}{4}$ and $P_{X|W=1}(1) = \frac{3}{4}$ then we say that X is ε -free (with respect to $\{W\}$) for $\varepsilon = \frac{1}{4}$.

We remark that a sequence of bits X_1, X_2, \dots for which each bit X_i is ε -free with respect to the previous ones is known in classical computer science as a Santha-Vazirani source [11].

III. MAIN RESULTS

The idea of the present work is to exploit a particular set of non-local correlations found in quantum theory that can be quantified using the chained Bell inequalities [12, 13]. If we have perfect free randomness to choose measurements, then the violation of a Bell inequality indicates that the measurement outcomes cannot be completely pre-determined [4]. Bell's arguments have recently been extended to show that, again under the assumption that we have perfect free randomness, there is no way to improve on the predictions quantum theory makes about measurement outcomes [10]. Here, we show that quantum correlations can be so strong that, even if we cannot choose the measurements perfectly freely, the outputs are nevertheless perfectly free.

To generate these correlations, we consider an experimental setup where local measurements are performed on a pair of maximally entangled qubits (see Figure 1). We first make the (temporary) assumption that quantum theory is correct, in the sense that the joint distribution of measurement outcomes is the one predicted by quantum theory for this setup. Crucially, however

we do not require completeness of quantum theory, i.e., that quantum theory is maximally informative about the measurement outcomes (for further discussion on the distinction between correctness and completeness, see Appendix A). Instead, we consider arbitrary additional parameters, modelled as a set of SVs, W , which may be provided by a higher theory. (Note that W can include measurement choices and outcomes of other systems that may not be classical.) Our first main result is the following theorem.

Theorem 1—For $\varepsilon < \frac{(\sqrt{2}-1)^2}{2} \approx 0.086$, $0 < \varepsilon' \leq \varepsilon$ and any (set of) SVs W , assuming correctness of quantum theory, there exists a protocol that uses ε -free bits with respect to W to generate ε' -free bits with respect to W .

The proof relies on a bipartite setup (see Figure 1). It is parameterized by an integer, N , corresponding to the number of measurement settings on each side. The SVs $A \in \{0, 2, \dots, 2N-2\}$ and $B \in \{1, 3, \dots, 2N-1\}$ correspond to measurement settings and $X \in \{+1, -1\}$ and $Y \in \{+1, -1\}$ are their respective outcomes. The measurements are made in such a way that the processes $A \rightsquigarrow X$ and $B \rightsquigarrow Y$ (this notation is defined precisely in Appendix B) are spacelike separated, and the entire process generates a probability distribution $P_{XY|AB}$. We introduce a measure of the strength of correlations by defining

$$I_N := P(X = Y|a_0, b_0) + \sum_{\substack{a,b \\ |a-b|=1}} P(X \neq Y|a, b), \quad (2)$$

where $a_0 = 0$ and $b_0 = 2N-1$ and $P(X \neq Y|a, b)$ is the probability that the measurements had different outcomes for settings $A = a$, $B = b$. This quantity was originally introduced to study *chained Bell correlations* [12, 13], and has found use in cryptography [14, 15] and quantum foundations [10, 16]. It turns out that all classical correlations satisfy $I_N \geq 1$, while quantum correlations exist for which

$$I_N = 2N \sin^2 \frac{\pi}{4N}, \quad (3)$$

which tends to 0 in the limit of large N (the state and measurements required to achieve this can be found in Appendix F).

In the proof of Theorem 1, we use the following lemma about no-signalling distributions. A bipartite conditional distribution $P_{XY|AB}$ is said to be *no-signalling* if $P_{X|AB} = P_{X|A}$ and $P_{Y|AB} = P_{Y|B}$ (a criterion which is readily generalized to more parties). The lemma then bounds the freedom of the output bits with respect to $\{A, B\} \cup W$ in terms of the strength of quantum correlations, quantified using I_N , and how free the measurement settings are, quantified via

$$q_N(a, b) := \min_{\substack{a', b', w' \\ |a' - b'| = 1}} \left[\frac{P_{W|a'b'}(w')}{P_{W|ab}(w')} \right].$$

Lemma 1—If $P_{XY|ABw}$ is no-signalling for all w , and $q_N(a, b) > 0$, then

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq \frac{I_N}{2q_N(a, b)} \quad (4)$$

for all a and b , where $P_{\bar{X}}$ denotes the uniform distribution on X .

The proof of this lemma is given in Appendix E.

Proof of Theorem 1—For $N = 2^r$, the measurement settings, A and B can be picked using r bits from the imperfect sources. Note that

$$q_N(a, b) = \min_{\substack{a', b', w' \\ |a' - b'| = 1}} \left[\frac{P_{AB|w'}(a', b')}{P_{AB|w'}(a, b)} \right]$$

in the case of uniform P_{AB} , which we can assume without loss of generality. For the sources described above, we have $q_{2^r}(a, b) \geq \left(\frac{1-2\varepsilon}{1+2\varepsilon} \right)^{2^r}$. Inserting this into (4) gives

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq \frac{I_{2^r}}{2} \left(\frac{1+2\varepsilon}{1-2\varepsilon} \right)^{2^r}.$$

Substituting the value of I_{2^r} obtainable in quantum theory (see Eq. (3)) gives

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq 2^r \left(\frac{1+2\varepsilon}{1-2\varepsilon} \right)^{2^r} \sin^2 \left(\frac{\pi}{2^{r+2}} \right).$$

Hence, using the bound $\sin x \leq x$ for $x \geq 0$, it follows that

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq \frac{\pi^2}{16} \left(\frac{1+2\varepsilon}{\sqrt{2}(1-2\varepsilon)} \right)^{2^r},$$

which tends to 0 as r tends to infinity provided $\varepsilon < \frac{(\sqrt{2}-1)^2}{2}$. Therefore, if the initial sources are ε -free, for such ε , then their outputs are arbitrarily free with respect to $\{A, B\} \cup W$ (and hence, in particular, with respect to W). \square

It is natural to ask whether the assumption made above, that quantum theory correctly predicts the correlations, is necessary, or whether, instead, the presence of sufficiently strong correlations can be certified using ε -free bits. This is also relevant in a cryptographic context, where the states and measurements are not trusted, and could have been chosen by an adversary with partial knowledge of the measurement settings (modelled by a set of SVs, W).

Theorem 2—For $\varepsilon < 0.0158$, $0 < \varepsilon' \leq \varepsilon$ and any (set of) SVs W , there exists a protocol that uses ε -free bits with respect to W to certify the generation of ε' -free bits with respect to W .

Certification means that the protocol involves a test of the correlations that is essentially impossible to pass unless the generated bits are ε' -free. However, the test is

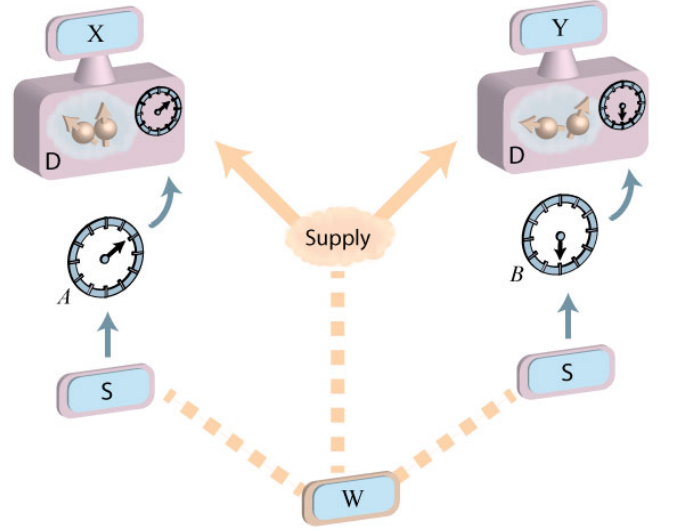


FIG. 1: **Illustration of the bipartite setup.** Spacelike separated measurements are carried out using devices denoted D. The measurement settings, A and B are derived from bits generated by two sources, denoted S . These bits are only partially free, i.e., they may be correlated (represented by the dashed line) with each other and with some other variables W (to be interpreted as parameters provided by a higher theory), which may also influence the supply of states being measured. By exploiting correlations between the outcomes X and Y , we show that, in spite of the lack of free randomness to choose settings, the outcome X is arbitrarily close to being uniform and uncorrelated with W .

passed if quantum theory is correct. The proof of Theorem 2 is given in Appendix F, where we describe and analyse a protocol that achieves this task.

Theorem 2 implies that there exists a device-independent protocol for free randomness amplification. Clearly this second scenario, where the assumption of correctness of quantum theory is dropped, is more demanding, hence the smaller range of ε for which free randomness amplification is successful. Nevertheless, the fact that it is possible at all is already fascinating.

It is an open question as to how far the threshold on ε can be pushed such that free randomness amplification remains possible (in either scenario). It turns out that using chained Bell correlations there is a limit, since (as shown in Appendix G) for $\varepsilon \geq \frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 0.146$, these correlations admit a local classical explanation. However, we conjecture that other protocols exist that use arbitrarily weak randomness to generate virtually perfect free randomness.

Conjecture 1—There exist alternative protocols such that the restriction on ε in Theorems 1 and 2 can be replaced by $\varepsilon < \frac{1}{2}$.

We give some evidence for this in Appendix H.

IV. DISCUSSION

We now discuss the implications of these results in light of previous work, starting with randomness extraction, introduced in [17, 18]. This is the task of taking a string of bits about which there may be some side information and using it to generate a string which is uniform even given this side information. All previous protocols for this task were classical and require an additional uniform random seed (i.e. bits which are perfectly free) which acts as a catalyst (there have recently been extensions of this work to certain imperfect seeds, provided they are uncorrelated with the string being compressed and that the size of the side information is bounded [19]). In the case without an independent seed, it has been shown that no classical algorithm can extract even a single uniform bit from an adversarially controlled string of partially free bits [11, 20]. This shows that free randomness amplification, which we show is possible in this work, cannot be done using only classical (deterministic) information processing. We give a more detailed discussion in Appendix D, where we also discuss the connection to independent sources of randomness, such as those in [21].

It is worth contrasting randomness amplification, as considered here, with *randomness expansion*, introduced in [22] and further developed in [23, 24]. There, an initial perfectly random finite seed is used within a protocol to generate a longer sequence of random bits using untrusted devices. In contrast, in the present work we do not require such a seed, but instead have an arbitrarily large supply of imperfect randomness.

A potential way to use our protocol is as a method for generating a seed, to be used with an extractor to extract further randomness from a partially free source, or to seed a randomness expansion protocol. Using Trevisan’s extractor [25, 26], for example, in the first case we could generate random bits at the entropy rate of the partially free source. In the second case, provided that the protocols can be securely composed, a secure randomness expansion protocol may allow a virtually unbounded amount of free randomness to be derived from a finite number of uses of partially free sources.

Our work also connects to the so-called “free will” theorem of Conway and Kochen [27, 28], which is, in essence, a combination of Bell’s theorem [4] and the Kochen-Specker theorem [29]. Conway and Kochen’s notion of free will is roughly the same as our definition of free ran-

domness. Hence, using their language, we could restate our main result as a proof that free will can be amplified.

We also comment on the implications of our result for experimental demonstrations of Bell-inequality violations. There are several potential loopholes in current experiments, leaving the door open for die-hards to reject certain philosophical implications. One such loophole, which has received only minor attention in the literature, is the so called *free-choice loophole*, which has been addressed in a recent experiment [30]. This loophole says that the supposedly free measurement settings were in fact known beforehand. In the aforementioned experiment, this is addressed by using random number generators, triggered at spacelike separation from the source of entangled pairs. However, as acknowledged in [30], this leaves room for what they call “super-determinism”, since it is impossible to exclude the possibility that the random number generator and the source of entanglement have interacted in the past.

Use of our result is also not able to close this loophole, and, since we can never rule out that the universe is deterministic, we don’t see any way to completely close it. Nevertheless, Theorem 2 allows the free choice assumption to be weakened: Instead of having to assume that the entanglement source and the random number generator are completely uncorrelated, we would only need to assume that they are not strongly correlated. Furthermore, if Conjecture 1 is correct, it is sufficient that they are not completely correlated. We therefore propose that, in experiments where the assumption of free choice is critical, these choices are generated using our free randomness amplification procedure.

Acknowledgements

We thank Viktor Galliard and Anthony Leverrier for useful discussions and comments, Lidia del Rio for Fig. 1 and Charles Bennett for bringing Ref. [21] to our attention. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. R.R. acknowledges support from the Swiss National Science Foundation (grant No. 200020-135048 and the NCCR QSIT) and from the European Research Council (grant No. 258932).

-
- [1] Bell, J. S. Free variables and local causality. In *Speakable and unspeakable in quantum mechanics*, chap. 12 (Cambridge University Press, 1987).
 - [2] de Finetti, B. La prevision: Ses lois logiques, ses sources subjectives. *Annales de l’Institut Henri Poincare* **7**, 1–68 (1937).
 - [3] Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nature Physics* **3**, 645–649

- (2007).
- [4] Bell, J. S. On the Einstein-Podolsky-Rosen paradox. In *Speakable and unspeakable in quantum mechanics*, chap. 2 (Cambridge University Press, 1987).
- [5] Kofler, J., Paterek, T. & Brukner, C. Experimenter’s freedom in Bell’s theorem and quantum cryptography. *Physical Review A* **73**, 022104 (2006).
- [6] Hall, M. J. W. Local deterministic model of singlet

- state correlations based on relaxing measurement independence. *Physical Review Letters* **105**, 250404 (2010).
- [7] Barrett, J. & Gisin, N. How much measurement independence is needed in order to demonstrate nonlocality? e-print [arXiv:1008.3612](#) (2010).
- [8] Hall, M. J. W. Relaxed Bell inequalities and Kochen-Specker theorems. e-print [arXiv:1102.4467](#) (2011).
- [9] Lorenzo, A. D. Free will and quantum mechanics. e-print [arXiv:1105.1134](#) (2011).
- [10] Colbeck, R. & Renner, R. No extension of quantum theory can have improved predictive power. *Nature Communications* **2**, 411 (2011).
- [11] Santha, M. & Vazirani, U. V. Generating quasi-random sequences from slightly-random sources. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS-84)*, 434–440 (1984).
- [12] Pearle, P. M. Hidden-variable example based upon data rejection. *Physical Review D* **2**, 1418–1425 (1970).
- [13] Braunstein, S. L. & Caves, C. M. Wringing out better Bell inequalities. *Annals of Physics* **202**, 22–56 (1990).
- [14] Barrett, J., Hardy, L. & Kent, A. No signalling and quantum key distribution. *Physical Review Letters* **95**, 010503 (2005).
- [15] Barrett, J., Kent, A. & Pironio, S. Maximally non-local and monogamous quantum correlations. *Physical Review Letters* **97**, 170409 (2006).
- [16] Colbeck, R. & Renner, R. Hidden variable models for quantum theory cannot have any local part. *Physical Review Letters* **101**, 050403 (2008).
- [17] Bennett, C. H., Brassard, G. & Robert, J.-M. Privacy amplification by public discussion. *SIAM Journal on Computing* **17**, 210–229 (1988).
- [18] Impagliazzo, R., Levint, L. A. & Luby, M. Pseudo-random generation from one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC-89)*, 12–24 (1989).
- [19] Kasher, R. & Kempe, J. Two-source extractors secure against quantum adversaries. In *Approximation, Randomization, and Combinatorial Optimization*, Lecture Notes in Computer Science, 656–669 (2010).
- [20] Dodis, Y., Ong, S. J., Prabhakaran, M. & Sahai, A. On the (im)possibility of cryptography with imperfect randomness. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS-04)*, Lecture Notes in Computer Science, 196–205 (2004).
- [21] Vazirani, U. V. Towards a strong communication complexity theory or generating quasi-random sequences from two communicating slightly-random sources. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing (STOC-85)*, 366–378 (1985).
- [22] Colbeck, R. *Quantum and Relativistic Protocols For Secure Multi-Party Computation*. Ph.D. thesis, University of Cambridge (2007). Also available as [arXiv:0911.3814](#).
- [23] Pironio, S. *et al.* Random numbers certified by Bell’s theorem. *Nature* **464**, 1021–1024 (2010).
- [24] Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *Journal of Physics A* **44**, 095305 (2011).
- [25] Trevisan, L. Extractors and pseudorandom generators. *Journal of the ACM* **48**, 860–879 (2001).
- [26] De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan’s extractor in the presence of quantum side information. e-print [arXiv:0912.5514](#) (2009).
- [27] Conway, J. & Kochen, S. The free will theorem. *Foundations of Physics* **36**, 1441–1473 (2006).
- [28] Conway, J. H. & Kochen, S. The strong free will theorem. *Notices of the AMS* **56**, 226–232 (2009).
- [29] Kochen, S. & Specker, E. P. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics* **17**, 59–87 (1967).
- [30] Scheidl, T. *et al.* Violation of local realism with freedom of choice. *Proceedings of the National Academy of Sciences USA* **107** (2010).
- [31] Colbeck, R. & Renner, R. Defining the local part of a hidden variable model: a comment. e-print [arXiv:0907.4967](#) (2009).
- [32] Greenberger, D. M., Horne, M. & Zeilinger, A. Going beyond Bell’s theorem. In Kafatos, M. (ed.) *Bell’s Theorem, Quantum Mechanics and Conceptions of the Universe*, 69–72 (Kluwer Academic, Dordrecht, The Netherlands, 1989).
- [33] Tsirelson, B. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement* **8**, 329–345 (1993).
- [34] Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Foundations of Physics* **24**, 379–385 (1994).
- [35] Broadbent, A. & Methot, A. On the power of non-local boxes. *Theoretical Computer Science* **358**, 3–14 (2006).

Appendix A: Correctness vs. completeness of quantum theory

For a large part of this work, we make the assumption that quantum theory is correct, but not necessarily complete. To recap, correctness means that the observed distributions of measurement outcomes will follow those given by quantum theory. Completeness is a stronger notion and means that there is no higher theory which better explains the outcomes (i.e., a theory that provides us with additional information allowing us to better predict the outcomes of measurements). While the correctness assumption is often sufficient, for instance, to predict the behaviour of a physical device, there are scenarios in which the additional assumption of completeness is crucial. One example is in quantum cryptography, which aims to show that there is no attack within the laws of physics that renders a cryptographic scheme insecure.

The distinction between these two notions is a significant one. Correctness is an operational concept and is in principle experimentally verifiable: by repeatedly measuring a system, we can place increasingly accurate bounds on

its statistics. Completeness, on the other hand, is not directly verifiable, and many of our experimentally well-founded theories have found higher explanation in the past (statistical mechanics explains many phenomena in thermodynamics at a higher level, for example). We therefore argue that assuming completeness is a different class of assumption, and we do not make it in this work.

Note that in the second part of our result, we also drop the assumption of correctness, showing that by performing measurements (chosen with ε -free bits) we can verify the correlations to a sufficient level to conclude that their outcomes are random.

Appendix B: General scenario and notation

Here we explain the setup of a general protocol for free randomness amplification. Before doing so, we introduce some notation.

A pair of SVs, (A, X) is said to be *time-ordered* (denoted $A \rightsquigarrow X$) if the coordinate (t, \mathbf{r}) of A lies in the backward lightcone of the coordinate (t', \mathbf{r}') of X , i.e. if $c^2(t - t')^2 \geq |\mathbf{r} - \mathbf{r}'|^2$ and $t \leq t'$ (where c is the speed of light). Furthermore, we say that two time-ordered pairs $A \rightsquigarrow X$ and $B \rightsquigarrow Y$ are *spacelike separated* if $A \not\rightsquigarrow Y$ and $B \not\rightsquigarrow X$.

We use W to summarize all parameters that a higher theory may provide. Using $\{R_j\}$ to denote the partially free bits, the requirements of Equation (1) imply that each bit R_j is ε -free with respect to $\{R_k\} \cup W$. In particular, $P_{R_j|W\Theta_j} \in [\frac{1}{2} - \varepsilon, \frac{1}{2} + \varepsilon]$ where Θ_j is the set of all bits R_k with time coordinate smaller than that of R_j (with respect to some reference frame).

We consider protocols for this task which involve performing M spacelike separated measurements $A_i \rightsquigarrow X_i$ for some $M \geq 2$. Each measurement setting, A_i , is derived from a number of bits R_j , and X_i is the corresponding outcome. The idea is that, for an appropriate distribution $P_{X_1 \dots X_M | A_1 \dots A_M}$ specified by the protocol (and realizable using a set of measurements on a quantum system prepared in a certain state), one or more of the output bits X_i , or some (possibly random) function of them, is arbitrarily close to being perfectly free.

We can also recast the setup in an adversarial scenario. Here, the set of variables, W , with which the partially free sources may be correlated can be thought of as being held by an adversary. (More generally, one could think of a correlated system (instead of the SVs W) which takes an input, corresponding to a choice of measurement, and gives an output (analogous to a quantum system). However, both the input and output can be included in the set W .) The adversary then supplies an M -party system whose behaviour, $P_{X_1 \dots X_M | A_1 \dots A_M w}$, may depend on W . For the first part of our result, we consider the case where the adversary sets up this system such that, if the partially free bits are used to choose $\{A_i\}$, the resulting distribution (averaged over W) is indistinguishable from that generated by performing quantum measurements on a quantum state specified by the amplification protocol. The only restriction for the adversary is that the distributions $P_{X_1 \dots X_M | A_1 \dots A_M w}$ are no-signalling. The output of the protocol is then considered free if it is uniformly distributed and the adversary is unable to learn anything about it.

Appendix C: Necessity of the no-signalling conditions

Here we show that, in order to incorporate perfectly free random bits into a theory, it is necessary that this theory satisfies the no-signalling conditions. Note that an M -party distribution $P_{X_1 \dots X_M | A_1 \dots A_M}$ is no-signalling if $P_{X_i^\perp | A_1 \dots A_M} = P_{X_i^\perp | A_i^\perp}$ for all i , where $X_i^\perp := X_1 \dots X_{i-1} X_{i+1} \dots X_M$. The argument essentially follows one proposed in [10] (see also [31]).

Lemma—Let A_i and X_i be a set of SVs such that $A_i \rightsquigarrow X_i$ are spacelike separated, where $i \in \{1, \dots, M\}$, and let W be an arbitrary set of SVs. If, for all i , A_i is perfectly free with respect to $W \cup \{A_j, X_j\}_j$, then $P_{X_1 \dots X_M | A_1 \dots A_M w}$ is no-signalling.

Proof—Using Bayes' rule we have

$$P_{X_i^\perp | A_1 \dots A_M w} = P_{X_i^\perp | A_i^\perp w} \frac{P_{A_i | A_i^\perp X_i^\perp w}}{P_{A_i | A_i^\perp w}}.$$

Since, by assumption, A_i is perfectly free with respect to $W \cup \{A_j, X_j\}_j$, and W , A_i^\perp and X_i^\perp are not in the future lightcone of A_i , we have $P_{A_i | A_i^\perp X_i^\perp w} = P_{A_i | A_i^\perp w} = P_{A_i}$. It hence follows that $P_{X_i^\perp | A_1 \dots A_M w} = P_{X_i^\perp | A_i^\perp w}$, i.e. that $P_{X_1 \dots X_M | A_1 \dots A_M w}$ is no-signalling.

Appendix D: Use of multiple independent sources

One may wonder whether, given the no-signalling assumption, the outputs of partially free sources at spacelike separation are necessarily independent of each other. If this was the case, i.e., if the sources were independent, it would be possible to generate arbitrarily free bits by a purely classical procedure. More precisely, as shown in [21], two independent sources of ε -free bits can be used to generate ε' -free ones for any $\varepsilon' > 0$ by taking as a final bit the number of places in which a sufficiently large number of the outputs are equal modulo 2 (the $\text{GF}(2)$ inner-product of the output strings).

In the following, we argue however that the no-signalling assumption does not generally imply that spacelike separated sources produce independent outputs. This is easily seen by example. Suppose that the separated sources share the quantum state

$$\left(\frac{1}{2} + \varepsilon\right) |00\rangle + \sqrt{\frac{1}{4} - \varepsilon^2} |01\rangle + \left(\frac{1}{2} - \varepsilon\right) |10\rangle + \sqrt{\frac{1}{4} - \varepsilon^2} |11\rangle$$

and generate their partially free bits by measurement in the $\{|0\rangle, |1\rangle\}$ basis. The resulting distribution corresponds in effect to choosing the bias of the second bit depending on the output of the first. However, by construction, this source of randomness is clearly no-signalling (because quantum theory has this property).

While the classical construction of [21] is not in general applicable to such correlated sources, our result shows that the partially free output of the sources can nevertheless be turned into almost perfectly free uniform randomness.

Appendix E: Proof of Lemma 1

We remark that this proof is a generalization of one given in [10], which in turn was based on a series of work [15, 16] going back to the first provably secure device-independent key distribution protocol [14].

Recall that we are working in a bipartite setup where measurements $A \rightsquigarrow X$ and $B \rightsquigarrow Y$ are made at spacelike separation, with $A \in \{0, 2, \dots, 2N - 2\}$, $B \in \{1, 3, \dots, 2N - 1\}$, $X \in \{+1, -1\}$ and $Y \in \{+1, -1\}$. We first consider the quantity I_N (defined in Equation (2)) evaluated for the conditional distribution $P_{XY|AB,w} = P_{XY|ABW}(\cdot, \cdot | \cdot, \cdot, w)$, for any fixed w . The idea is to use this quantity to bound the trace distance between the conditional distribution $P_{X|aw}$ and its negation, $1 - P_{X|aw}$, which corresponds to the distribution of X if its values are interchanged. If this distance is small, it follows that the distribution $P_{X|aw}$ is roughly uniform.

For $a_0 = 0$, $b_0 = 2N - 1$, we have

$$\begin{aligned} I_N(P_{XY|AB,w}) &:= P(X = Y|a_0, b_0, w) + \sum_{\substack{a,b \\ |a-b|=1}} P(X \neq Y|a, b, w) \\ &\geq D(1 - P_{X|a_0 b_0 w}, P_{Y|a_0 b_0 w}) + \sum_{\substack{a,b \\ |a-b|=1}} D(P_{X|abw}, P_{Y|abw}) \\ &= D(1 - P_{X|a_0 w}, P_{Y|b_0 w}) + \sum_{\substack{a,b \\ |a-b|=1}} D(P_{X|aw}, P_{Y|bw}) \\ &\geq D(1 - P_{X|a_0 w}, P_{X|a_0 w}) \\ &= 2D(P_{X|a_0 w}, P_{\bar{X}}), \end{aligned} \tag{E1}$$

where we have used the no-signalling conditions $P_{X|abw} = P_{X|aw}$ and $P_{Y|abw} = P_{Y|bw}$, the triangle inequality for D and the relation $D(P_{X|\Omega}, P_{Y|\Omega}) \leq P(X \neq Y|\Omega)$ for any event Ω .

Since the quantity $I_N(P_{XY|AB,w})$ cannot be computed without access to w , we instead consider

$$\begin{aligned}
I_N(P_{XY|AB}) &:= P(X=Y|a_0, b_0) + \sum_{\substack{a,b \\ |a-b|=1}} P(X \neq Y|a, b) \\
&= \sum_w P_{W|a_0 b_0}(w) P(X=Y|a_0 b_0 w) + \sum_{\substack{a,b \\ |a-b|=1}} \sum_w \frac{P_{W|ab}(w)}{P_{W|a_0 b_0}(w)} P_{W|a_0 b_0}(w) P(X \neq Y|abw) \\
&\geq \sum_w P_{W|a_0 b_0}(w) \min_{\substack{a,b,w \\ |a-b|=1}} \left[\frac{P_{W|ab}(w)}{P_{W|a_0 b_0}(w)} \right] I_N(P_{XY|ABw}) \\
&\geq 2 \min_{\substack{a,b,w \\ |a-b|=1}} \left[\frac{P_{W|ab}(w)}{P_{W|a_0 b_0}(w)} \right] D(P_{XW|a_0 b_0}, P_{\bar{X}} \times P_{W|a_0 b_0}). \tag{E2}
\end{aligned}$$

Using the definition of $q_N(a, b)$, we have the bound

$$D(P_{XW|a_0 b_0}, P_{\bar{X}} \times P_{W|a_0 b_0}) \leq \frac{I_N(P_{XY|AB})}{2q_N(a_0, b_0)}.$$

The proof for arbitrary a and b (rather than $a = a_0, b = b_0$) follows by symmetry.

Appendix F: Proof of Theorem 2

Note that the bounds used in this section are not tight and one would expect to be able to improve the bound we give on ε ; our aim here is to give a proof-of-principle. The protocol we use for free randomness amplification is in essence a one-party version of the Barrett-Hardy-Kent key distribution protocol [14]. The quantum correlations we rely on are those formed by measurements on the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in the bases $\{\cos \frac{\theta_a/b}{2} |0\rangle + \sin \frac{\theta_a/b}{2} |1\rangle, \sin \frac{\theta_a/b}{2} |0\rangle - \cos \frac{\theta_a/b}{2} |1\rangle\}$, where $\theta_a = \frac{\pi a}{2N}$ and $\theta_b = \frac{\pi b}{2N}$. Note that although we phrase the protocol in terms of measurements on maximally entangled states, we do not have to trust that this is what is actually happening. The protocol is based only on the observed correlations. It involves two parameters, M and N , to be determined later.

1. Take M maximally entangled qubit pairs and isolate each qubit (for example, all of the qubits could be spacelike separated).
2. For each pair, pick $A_q \in \{0, 2, \dots, 2N-2\}$ randomly using $\log N$ instances from a source of ε -free bits, and likewise pick $B_q \in \{1, 3, \dots, 2N-1\}$. Make the corresponding measurement and record the outcomes ($X_q \in \{0, 1\}$ and $Y_q \in \{0, 1\}$).
3. Collect the choices A_q and B_q and discard all rounds except those for which A_q and B_q were neighbouring.
4. Collect X_q and Y_q for all the remaining pairs (call this set \mathcal{S}). If the size of \mathcal{S} is not between M/N and $M/N^{3/4}$, abort.
5. Pick one of the members, f , of \mathcal{S} (randomly using an ε -free source).
6. For each member of \mathcal{S} , check that $X_q = Y_q$ ($X_q \neq Y_q$ for $A_q = 0, B_q = 2N-1$). If this condition does not hold for any q , then abort.
7. Use X_f as the final free bit.

We sketch the proof that this protocol is secure. We say that the protocol fails if the marginal distribution $P_{X_f Y_f | A_f B_f w}$ on round f has $I_N(P_{X_f Y_f | A_f B_f w}) > I_N^*$, for some positive real number I_N^* , to be specified later, and it doesn't abort. The idea is to show that the protocol fails with low probability, i.e. for any non-signalling distribution with a significant probability that $I_N(P_{X_f Y_f | A_f B_f w}) > I_N^*$, there is a high probability of the protocol aborting in Step 6.

For each marginal distribution with $I_N > I_N^*$, in the worst case, there is one pair (A, B) that could potentially lead to detection (the resulting detection probability is then at least I_N^*), and this pair is chosen with probability $(1/2 - \varepsilon)^{2 \log N}$. For simplicity, we use that the other neighbouring pairs are each chosen with probability at most $(1/2 + \varepsilon)^{2 \log N}$.

There are at least M/N neighbouring pairs (otherwise the protocol aborts). From the set of neighbours, ε -free bits are used to pick the final outcome. The most probable choice occurs with probability $(1/2 + \varepsilon)^{\log(M/N)} = (M/N)^{\log(1/2+\varepsilon)}$, so the typical set has at least $(M/N)^{-\log(1/2+\varepsilon)}$ members.

A significant fraction of this typical set must have $I_N > I_N^*$ for the protocol to fail. For each member of the typical set with $I_N > I_N^*$, the probability that it is measured using the (A, B) pair that enables detection is at least $\frac{(1/2-\varepsilon)^{2 \log N}}{2N(1/2+\varepsilon)^{2 \log N}}$. The average number of times that the condition in Step 6 does not hold thus scales as

$$(M/N)^{-\log(1/2+\varepsilon)} N^{-1-2 \log(1/2+\varepsilon)+2 \log(1/2-\varepsilon)} I_N^*$$

(recall that if this condition does not hold, the protocol aborts).

If we choose $M = N^{5/2}$ and $I_N^* = N^{-1/4}$ and substitute into the above, we get $N^{-7/2 \log(1/2+\varepsilon)+2 \log(1/2-\varepsilon)-5/4}$, whose exponent is positive for $\varepsilon < 0.0158$, and hence this value grows with N for small enough ε . Note that, since the value of I_N^* can be made arbitrarily small, it follows using the relation (E1) (which, by symmetry holds with a_0 replaced by arbitrary a) that ε' can also be made arbitrarily small.

Note also that quantum correlations can achieve a value of I_N that scales like $1/N$, so that, with the above choice of M , the average number of detections in the case with perfect quantum states scales like $N^{-1/2}$, which tends to 0 for large N . Thus, the protocol will almost never abort if correctly implemented with quantum states.

Appendix G: Limitation of using chained Bell correlations

In the following we show that, using the above approach based on chained Bell correlations, the threshold on ε in Theorem 1 cannot be made arbitrarily small. To do so, we prove that if ε is above a certain value, then these correlations admit a classical explanation.

We first note that a classical strategy can always appear to satisfy the correlations (lead to a measured value of $I_N = 0$) if one pair of A, B values present in the definition of I_N is known not to occur. Furthermore, using the best possible classical strategy, for each $W = w$, either $P(X = Y|a_0, b_0, w)$ or one of $\{P(X \neq Y|a, b, w)\}_{|a-b|=1}$ will equal 1 and all the others will be 0. Therefore, the optimal classical strategy involves a setup in which the term that equals 1 corresponds to the pair (a, b) with the minimum probability of occurring, which can be set using W . For $N = 2^r$, we have $\min_{a,b} P_{AB|w}(a, b) = (\frac{1}{2} - \varepsilon)^{2r}$ and we assume the minimal pair is chosen uniformly over the pairs (a, b) in I_N (this makes it easiest to recreate the correlations using a classical strategy, i.e., in a cryptographic picture, it gives the greatest power to the adversary). We hence have

$$\begin{aligned} P(X \neq Y|a, b) &= \sum_w P(X \neq Y, W = w|a, b) \\ &= P(W = (a, b)|a, b) \\ &= \frac{P(W = (a, b))P(a, b|W = (a, b))}{P(a, b)} \\ &= \frac{2^{-(r+1)}(\frac{1}{2} - \varepsilon)^{2r}}{2^{-2r}} = 2^{r-1} \left(\frac{1}{2} - \varepsilon\right)^{2r} \end{aligned}$$

for $(a, b) \neq (a_0, b_0)$, and the same value is obtained for $P(X = Y|a_0, b_0)$. (Here $W = (a, b)$ indicates the pair of a and b values that are least likely to occur.) The value of I_{2^r} that would be observed is then $(1 - 2\varepsilon)^{2r}$.

In order to be consistent with quantum theory, this should be at most $2^{r+1} \sin^2 \frac{\pi}{2^{r+2}}$, i.e.

$$\frac{1}{2} - \varepsilon \leq \frac{1}{\sqrt{2}} \left(2 \sin^2 \frac{\pi}{2^{r+2}}\right)^{\frac{1}{2r}}.$$

This function is decreasing in r , so, in order to achieve arbitrarily free output bits with the largest ε , we should use the largest possible r . For large r , the right hand side approaches $\frac{1}{2\sqrt{2}} \left(\frac{\pi^2}{8}\right)^{\frac{1}{2r}}$, hence, in the limit $r \rightarrow \infty$, consistency with quantum theory is achievable for $\varepsilon \geq \frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 0.146$.

The above places limitations on when free randomness amplification is possible using chained Bell correlations (we cannot expect to improve the quality of bits from sources of ε -free bits with $\varepsilon \geq 0.146$, using these correlations). Note that related limitations on using bipartite correlations (in the context of demonstrating non-locality) have been reached in other recent work [5–8].

Appendix H: Possible route to proving Conjecture 1

We hint that one may be able to establish the truth of Conjecture 1 using GHZ states [32]. That GHZ correlations may be more useful for this task comes from the following observations about GHZ correlations: for any $0 \leq \varepsilon < \frac{1}{2}$, ε -free bits are sufficient to demonstrate non-locality for these correlations (in contrast to the bipartite case, whose limitations were described above). We first outline a few important properties of these correlations.

For M parties, GHZ correlations are those generated by measuring each part of the state $\frac{1}{\sqrt{2}}(|0 \dots 0\rangle - |1 \dots 1\rangle)$ in either the $\{|+\rangle_x, |-\rangle_x\}$ or $\{|+\rangle_y, |-\rangle_y\}$ basis (where $|\pm\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|\pm\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$). For convenience, we denote the inputs corresponding to these bases 0 and 1 respectively. These correlations have the property that certain output combinations are impossible. For example, if $M = 3$ and all three parties input 0 the product of the outcomes is always -1 . We now consider a classical strategy, which corresponds to an assignment of outputs to each input (this assignment may depend on some additional SVs, W). We label the bits assigned to the i th output by $x_i^0 \in \pm 1$ and $x_i^1 \in \pm 1$, where the superscript refers to the possible inputs $A_i = 0$ or $A_i = 1$.

In order to mimic the quantum correlations, the classical output bits need to satisfy $x_1^0 x_2^0 x_3^0 = -1$, $x_1^0 x_2^1 x_3^1 = 1$, $x_1^1 x_2^0 x_3^1 = 1$ and $x_1^1 x_2^1 x_3^0 = 1$. It is easy to see that this is impossible (for example, taking the product of all three equations yields $(x_1^0 x_2^0 x_3^0 x_1^1 x_2^1 x_3^1)^2 = -1$). However, there are classical strategies which satisfy 3 of these relations (for example, when each output is 1, independent of its input).

We now imagine choosing measurements to perform on tripartite GHZ states using bits that are ε -free. As mentioned above, for any classical strategy, there is at least one combination of inputs that yields an incorrect set of outputs. Using the ε -free source of randomness in three places, the probability of such an input is $(\frac{1}{2} - \varepsilon)^3$. Hence, for any $\varepsilon < \frac{1}{2}$, the presence of a classical strategy will eventually be noticed as more tests are performed. We conclude that non-locality can be verified with ε -free bits provided $\varepsilon < \frac{1}{2}$ (i.e. the bits are not completely correlated with W).

Nevertheless, it does not follow that the outputs of such measurements are completely free, and, in fact, it is easy to see that they may not be. One set of no-signalling correlations that satisfy all the GHZ relations is realized by having a deterministic output (conditioned on W) for one of the parties, and a non-local box [33, 34] shared between the remaining two [35]. Using these correlations, there is always one output that is deterministic and hence not free and random.

However, we suggest that arbitrarily free bits may be generated from partially free ones using an M -party GHZ state for large M . The partially free source of randomness is used in M places to choose measurements on each part of the state in either of the two bases specified above. Then, if the outputs satisfy the M -party GHZ relations, one of the randomness sources is used to pick one of the M output bits at random. The idea is that, in the limit of large M , this output is arbitrarily close to being perfectly free, except with very small probability. However, it may turn out that other states and measurements are required in order to prove Conjecture 1.

A corollary of the above is that if the measurement devices are restricted to be quantum (rather than arbitrary no-signalling, i.e. we trust that the measurement devices are limited by quantum theory, but not what they are doing internally), ε -free bits for any $0 \leq \varepsilon < \frac{1}{2}$ can be used to generate arbitrarily free bits. This follows from the observation that the only quantum states that perfectly obey the tripartite GHZ relations are (up to local unitary operations) GHZ states [22, 24], from which perfect randomness can be derived by taking any of the three outputs. Hence, a set of quantum measurement devices that never deviate from the GHZ relations (using measurements chosen with an ε -free source) also generate perfectly free randomness.
